International Journal of Scientific Research and Engineering Development-– Volume 5 Issue 6, Nov- Dec 2022

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Artificial Intelligence and its Impact on Cyber Security

Ribence Kadel[1], Riya Kadel[2]

(ribence.kadel456@gmail.com)[1]

(riya.kadel345@gmail.com)[2]

----------**********----------

Abstract:

Not only has the frequency of cyberattacks risen substantially over the previous few decades, but they have also become more sophisticated. As a result, developing a cyber-resilient strategy is critical. Traditional security solutions are insufficient to prevent data breaches in the event of a cyberattack.Cybercriminals have learnt how to hack, attack, and breach data using new tactics and powerful tools. Fortunately, AI technologies have been introduced into cyberspace to build smart models for safeguarding systems from threats. AI technologies may be employed as important tools in the realm of cybersecurity since they can rapidly adapt to solve complicated scenarios.AI-based solutions have the potential to deliver fast and strong cyber defense tools for recognizing malware assaults, network intrusions, phishing and spam emails, and data breaches, to mention a few, and alerting security problems when they occur. On this study, we examine the influence of artificial intelligence (AI) in cybersecurity and outline existing studies on the procedures, benefits and drawbacks of AI in cybersecurity.

Keywords: Artificial Intelligence (AI), phishing, malware, cyber defense tools, machine learning, deep learning

----------**********----------

1. Introduction

The exponential rise of computer networks has resulted in a massive increase in the number of cyberattacks. Every aspect of our society, from governance to the business to key infrastructure, is affected.

Infrastructures are heavily reliant on computer networks and information technologies. As a result, they are clearly vulnerable to cyberattacks. A cyberattack is defined as an assault undertaken by one or more computers against other computers or networks. The purpose of a cyberattack is often to either disable the target computer, take the services offline, or get access to the target computer's data.Since the first denial-of-service (DOS) attack in 1988, the frequency and severity of cyberattacks have grown dramatically. Indeed, cybersecurity has become one of the most difficult challenges in the area of computer science, and the quantity and sophistication of cyberattacks are predicted to expand continuously and rapidly.

Traditional cybersecurity approaches focus on static control of security equipment and work in reaction to an attack. For example, in the event of a network intrusion assault, security systems monitor nodes based on a predefined set of criteria. These approaches await notification that an assault has happened. The old strategy, however, is no longer effective in light of the rising number of cyberattacks. The Equifax attack in 2017, which exposed private information for up to 143 million consumers, is one illustration of the inadequacies of typical cybersecurity approaches. Furthermore, with new threat techniques such as advanced persistent threats (APTs) and zero-day attacks, attackers typically conceal their activities and attacks occur before software developers discover the vulnerabilities; as a result, it takes a significant amount of time to repair the vulnerable systems.

AI in cybersecurity offers tremendous benefits, but it also poses significant hurdles, as does any sophisticated general-purpose, dual-use technology. AI can help with cybersecurity and defense.AI in the form of ML and deep learning will intensify sophisticated assaults, allowing for quicker, more focused, and damaging attacks. The use of AI in cybersecurity raises security and ethical problems. Among other things, it

is unclear how duties for autonomous response systems should be assigned, how to ensure that systems behave as expected, or what the security threats posed by the rising anthropomorphizing of AI systems.

2. AI systems' support to cybersecurity

Enterprises have begun to use AI to handle a widening spectrum of cybersecurity threats, technological obstacles, and resource restrictions by improving the robustness, resilience, and reaction of their systems. Police dogs are a good model for why businesses are utilizing AI to improve cybersecurity. Police personnel employ the specialized talents of police dogs to seek dangers; similarly, AI systems collaborate with security analysts to modify the pace at which operations may be completed. In this sense, the interaction between AI systems and security operators should be viewed as a synergistic integration in which both people and AI systems' distinctive added value are retained and increased, rather than as a competition between the two.The market for AI in cybersecurity is expected to expand from $3.92 billion in 2017 to $34.81 billion by 2025, at a compound annual growth rate (CAGR) of 31.38% during the forecast period. According to a recent Capgemini report, the adoption rate of AI solutions for cybersecurity is rapidly increasing. From one-fifth of the general sample in 2019, to two-thirds of firms planned to deploy them in 2020, the number of organizations using these systems has increased. In cybersecurity, 73% of the sample tried AI applications. Network security is the most common application, followed by data security and endpoint security. There are three major categories of AI use in cybersecurity: detection (51%), prediction (34%), and response (18%).

2.1 System Robustness

Robustness is defined as a system's ability to withstand perturbations that fundamentally alter its configuration. To put it another way, a system is robust when it can continue to function in the face of internal or external challenges without changing its original configuration.System resilience requires that AI can discover and profile anomalies in anything that is generally distinct. It should be emphasized, however, that when sophisticated attackers hide by blending in with regular observed behaviors, this strategy might generate a lot of noise from benign detections and false negatives. As a result, more robust and accurate approaches concentrate on detecting specific and immutable attacker behaviors.

Another use for increasing system resilience is code review. Peer code review is a typical best practice in software engineering in which source code is manually examined by peers.

By automating the process using AI technologies, you may save time while also discovering more faults than you could manually. Several AI algorithms are being developed to aid with code review. For example, in June 2020, Amazon Web Services' AI-powered code reviewer from CodeGuru became publicly available.

The use of AI to improve system resilience has both tactical and strategic implications (i.e., enhancing system security and lowering susceptibility). It does, in fact, mitigate the impact of zero-day attacks. Zero-day attacks take advantage of vulnerabilities that are exploitable by attackers as long as system providers are unaware of them or there is no patch to address them. AI reduces the impact of zero-day attacks on the black market, lowering their value.

2.2 System Resilience

Resilience is defined as a system's capacity to withstand and endure an assault by facilitating threat and anomaly detection. In other words, a system is resilient if it can respond to internal and external obstacles by modifying its operational procedures while remaining operational. Unlike system robustness, system resilience entails a fundamental shift in the essential processes of the system that must adapt to the new environment. TAD (threat and anomaly detection) is the most prevalent use of AI systems nowadays. Every day, about 592,145 new unique malware files are created, with the possibility of even more.

AI cybersecurity solutions enable a fundamental change away from signature-based detection and toward more flexible and continuous monitoring of the network when it deviates from its typical behavior. "AI systems can detect any changes that seem abnormal - without the necessity for a predefined definition of abnormal." Deep packet traces performed by internal or external sensors or monitoring software can provide give information into prospective assaults.

AI is used by businesses to automate cyber defenses against spam and phishing, as well as to identify malware, fraudulent payments, and compromised computers and network systems.
AI is also applied in key forensics and investigation procedures. AI is utilized in particular to provide real-time, customer-specific analysis, increasing the total percentage of malware found and decreasing false positives. As a result, AI data processing aids in the improvement of cybersecurity threat intelligence. Finally, organizations are employing AI-based predictive analytics to evaluate the likelihood of attacks, hence improving network defense through near real-time data provision. Predictive analytics may assist in processing real-time data from many sources and detecting attack vectors by assisting in large data management; filtering and parsing data before analysis; and automatically filtering out duplicates.

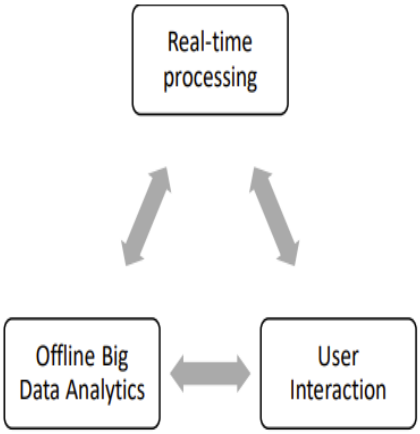
2.3 System Response

System resilience and response are inextricably linked and logically interdependent, because in order to respond to a cyberattack, you must first detect what is happening and then develop and deploy an appropriate response by deciding which vulnerability to attack and when, or by launching counterattacks. Seven AI systems competed in the 2014 Defense Advanced Research Projects Agency (DARPA) Cyber Grand Challenge, detecting and repairing their own vulnerabilities while exploiting their opponents' faults without human intervention. Since then, cyberattack prevention has shifted toward systems that can deploy real-time fixes to security problems. AI can assist in reducing the workloads of cybersecurity specialists by prioritizing areas that require more attention and automating parts of the experts' activities. This is especially important when one considers the current shortage of cybersecurity professionals, which is estimated to be four million workers.

AI can aid in assault response by, for example, deploying semi-autonomous lures that generate a replica of the environment that the attackers plan to enter. These fool them and aid in understanding the payloads (the attack components in charge of carrying out an action to hurt the target). AI systems may also dynamically divide networks to isolate assets in restricted network zones or redirect an attack away from vital data. Furthermore, AI systems may develop adaptive honeypots (computer systems designed to resemble plausible targets of assaults) and honeytokens (data chunks that appear appealing to potential attackers). Adaptive honeypots are more complicated than regular honeypots in that they adapt their behavior in response to attacker interactions. It is feasible to deduce the attacker's skills and tools based on its reaction to the defenses. The AI solution learns the attacker's behavior using this tool so that it may be recognized and countered in future attempts.

2.4 Major Techniques in the Use of Ai for System Robustness, Resilience, and Response

Whenever AI is applied to cyber-incident detection and response the problem solving can be roughly divided into three parts, as shown below. Data is collected from customer environments and processed by a system that is managed by a security vendor. The detection system flags malicious activity and can be used to activate an action in response.

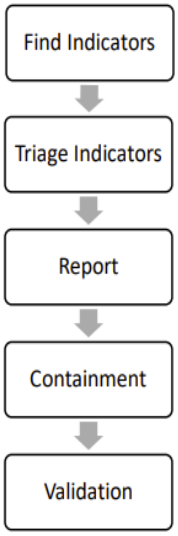


Source: Palo Alto Network contribution to the fourth meeting of the CEPS Task Force.

Companies today recognize that the attack surface is growing massively because of the adoption of the Internet of Things (IoT) and the diffusion of mobile devices, compounded by a diverse and ever-changing threat landscape. Against this backdrop, there are two measures that can be implemented: speed up defenders, slow down attackers.

Companies use AI solutions to automate the detection and response to threats that are already active within the organization's defenses in order to speed up defenders. Traditionally, security teams have spent a significant amount of time dealing with alerts, determining if they are benign or malicious, reporting on them, containing them, and confirming the containment steps. Some of the activities that security operations teams spend the majority of their time on can be assisted by AI.

Notably, this is also one of the keys and most widespread applications of AI in general.



The questions security team can use are the maturity, scale, method of exploit, actions and behavior manifestation of the attack.

3. Advantages of AI in Cyber Security

- Machine learning (ML) trained on immutable attacker 'Tactics, Techniques, and Procedures' (TTP) behaviors (as identified in the Mire Attack framework) can support long-term and broad attacker detection.
- ML based on user interaction provides a method of understanding local context and determining which data to focus on; models trained to detect those more likely to be harmful increase system performance by triaging the information to process in real time. Using ML in this manner not only saves money but also enables for speedier response in the most crucial situations.
- By developing robust models from the data, it is fed, ML can be effective in spotting new abnormalities. ML is especially adept at detecting patterns and extracting algorithms from enormous amounts of data in which humans are absent.
- Asynchronous user profiling and measuring deviation from common behaviors, as well as going back to much larger data volumes to understand behavior, can all benefit from machine learning.
- Vulnerability management may be aided by analyzing and assessing existing security measures using AI Investigations. AI enables you to analyze systems faster than cybersecurity experts, enhancing your problem-solving abilities significantly.
- AI takes care of redundant cybersecurity operations that might weary your cybersecurity worker while imitating the best of human traits and leaving out the flaws. It aids in the detection and prevention of fundamental security risks on a regular basis. It also does a thorough analysis of your network to check if there are any security flaws that might be harmful to your network.

4. Drawbacks of AI on Cyber Security

- Organizations would require far more resources and financial commitments to create and operate an AI system.
- Because AI systems are taught utilizing data sets, businesses need to collect a variety of malware, non-malicious code, and anomaly sets. Obtaining all of these data sets is time-consuming and expensive, which most businesses cannot finance.
- AI systems can provide erroneous findings and/or false positives in the absence of large amounts of data and events. Obtaining incorrect data from untrustworthy sources might sometimes backfire.
- Hackers may utilize AI to evaluate their malware and conduct more sophisticated assaults.

References:

W.L. Al-Yaseen, Z.A. Othman, M.Z.A. Nazri, “Multilevel hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system,”. Expert Syst. Appl. 2017, 67, 296-303.

Katanosh Morovat, Brajendra Panda, “A SURVEY OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY,”.2020 International Conference on Computational Science and Computational Intelligence (CSCI).

https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

Lorenzo Pupillo, Stefano Fantin, Afonso Ferreira, Carolina Polito, “Artificial Intelligence and Cybersecurity Technology, Governance and Policy Challenges Final Report of a CEPS Task Force.”

K. Skapinetz (2018), “Overcome cyber security limitations with artificial intelligence”, June (www.youtube.com/ watch?time_continue=10&v=-tIPoLin1WY&feature=emb_title)

Markets and Markets, “Artificial Intelligence in Cybersecurity Market by Technology Machine Learning, Context Awareness - 2025”, Markets and Markets (www.marketsandmarkets.com/Market-Reports/ai-in-cybersecuritymarket-224437074.html)

CAP Gemini (2019), "Reinventing Cyber security with Artificial Intelligence. The new frontier in digital security", Research Institute.
Amazon, Code Guru (https://aws.amazon.com/it/codeguruM. Taddeo T. McCutcheon and L. Floridi (2019), "Trusting artificial intelligence in cybersecurity is a double-edged sword", Nature Machine Intelligence, November, pp. 1-4./).
Palo Alto Network's contribution to the fourth meeting of the CEPS Task Force.
R. Goosen et al. (2018), "Artificial intelligence is a threat to cybersecurity. It's also a solution", The Boston Consulting Group.
Ibid.
Whois XML API (2019), "The importance of Predictive Analytics and Machine Learning in Cyber security", Circle ID, September
(2019), "Cybersecurity Workforce Study Strategies for Building and Growing Strong Cybersecurity Teams" (www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-WorkforceStudy-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482).
Ibid.
S. Dilek, H. Caku and M. Aydin, (2015), "Applications of Artificial Intelligence Techniques to Combating Cyber Crime: A Review", International Journal of Artificial Intelligence & Applications, p. 24.https://www.analyticssteps.com/blogs/6-advantages-ai-cyber-security

